Attacking WPA/WPA2 Enterprise Networks

By W1red

Introduction: This guide will discuss some of the security flaws regarding wireless networks implementing WPA/WPA2 Enterprise authentication as well as ways to exploit these weaknesses. Enterprise type authentication models are mostly used in corporate settings consisting of companies that typically have a lot of people. From what I have seen a lot of Universities, Colleges as well as Hospitals also use this form of authentication to verify its users. The methods discussed below are usually a result of VERY COMMON poor configuration in regards to certificate validation as well as RADIUS configuration.

DISCLAIMER: DO NOT USE ANY OF THE METHODS BELOW AGAINST NETWORKS THAT YOU ARE NOT AUTHORIZED TO AUDIT.

Homework: First and foremost if you do not know exactly how enterprise authentication works I suggest you do some reading to get yourself familiar with the process of how clients are verified. I highly suggest reading this PEAP which discussed the different types authentication types that can take place within enterprise. Also take a look at RADIUS which gives some nice detail as to how the RADIUS server works.

A few things to take note of:

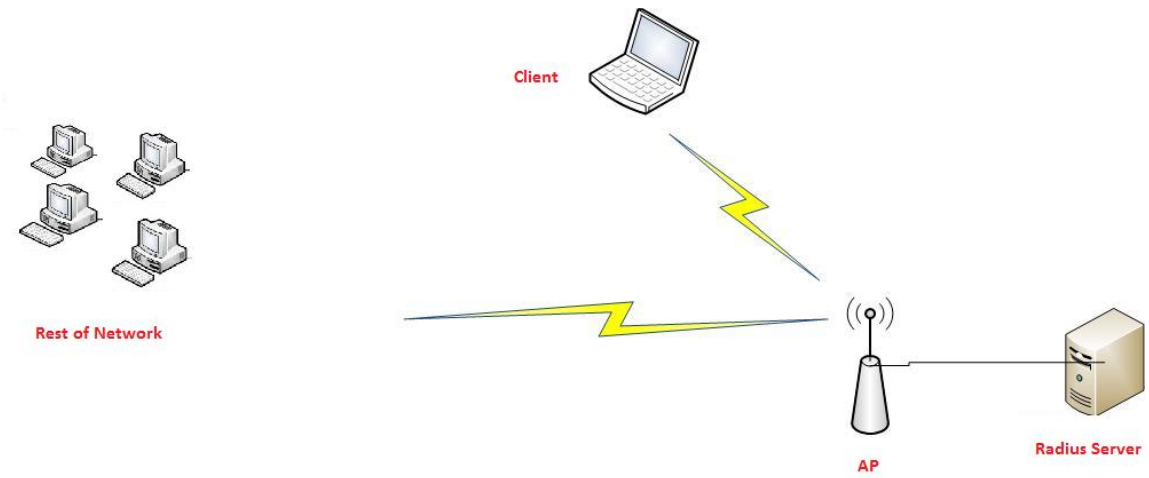
1. WPA/WPA2 Enterprise does NOT use a preshared key, this means that every time a user is verified on the network a random key is generated. To the best of my knowledge this cannot be cracked by capturing packets.

2. This guide will cover mainly PEAP since it accounts for 80% or more of the types used in the US (see Wikipedia page)

3. EAP is responsible for authentication NOT the access point

4. The access point handles the encryption(TKIP/CCMP)

I will try and outline how the authentication process works as simply as possible...



Okay, this diagram will hopefully help you visualize what's going on. Here is the process in order which things occur....

1.Client sends request to access point to connect.
2. The access point responds telling the client to connect to the RADIUS server to be authenticated.
3. Client connects to the RADIUS server.
4. RADIUS sets up TLS tunnel to receive username and password from client.
4. RADIUS server verifies client .
5. RADIUS server tells access point that the client is verified and can now connect.

Scenario 1:

For our first attack we will be using a rogue access point. Due to the way enterprise is implemented this becomes essential in helping us get past the RADIUS server problem. The Radius server uses a certificate to validate the access point along with the network. Once the certificate is validated the client sends his username and password to the server to be verified. What we will be exploiting is a VERY common mistake made in configuring PEAP, where certificate validation is NOT used! If PEAP is configured this way (surprisingly a lot of the time it is..) the client will not be prompted if an invalid certificate is used and unknowingly will accept it.

Step 1: Create a fake AP by matching the target networks SSID, encryption type and band (a/b/g/n).

This can very simple or very complex depending on how sophisticated you want this attack to be. For example you could take a regular Linksys home router change its settings and run it off of batteries for more stealth placement. See this link for details on running a router off of batteries Wrt54g on batteries. You can run a normal Linksys router on a lead acid battery for close to a month.

This allows for stealthy placement of the access point where it will not need a hard wired power source. Using modified antennas and/or amplifies will also be more powerful in getting users to connect. (more info on this later)

Step 2: Create our own fake RADIUS server.

Okay we have our fake access point that identical to our target network. Now we need our fake RADIUS server. We will be setting up our own little fake RADIUS server on a version of Backtrack4 which will be connected wirelessly to our fake access point. Download the free radius server from www.freeradius.org (You may need version 2.02 haven't tested with the newer one) . Extract freeRADIUS and go to that directory. We will be applying a patch known as Wireless Pwnage Edition created by Joshua Wright and Brad Antoniewicz. Available here WPE freeradius.

What this patch does:

- Will return success for ANY authentication request regardless of who it is.
- Will create a Log of all client credentials. This includes username, password and the challenge response. (if you don't know what a challenge response is you didn't read the Wikipedia page)
- This will log credentials for PEAP, TTLS, LEAP, EAP-MD5, EAP-MSCHAPv2,PAP,CHAP

In the directory where freeRadius is extracted run the following to patch freeRADIUS.

```
$ patch -p1 < ../freeradius-wpe-2.0.2.patch
$ ./configure && make && sudo make install && sudo ldconfig
```

Now we will create our certificates.

```
$ cd freeradius-server-2.0.2/raddb/certs
$ ./bootstrap
$ sudo cp -r * /usr/local/etc/raddb/certs
```

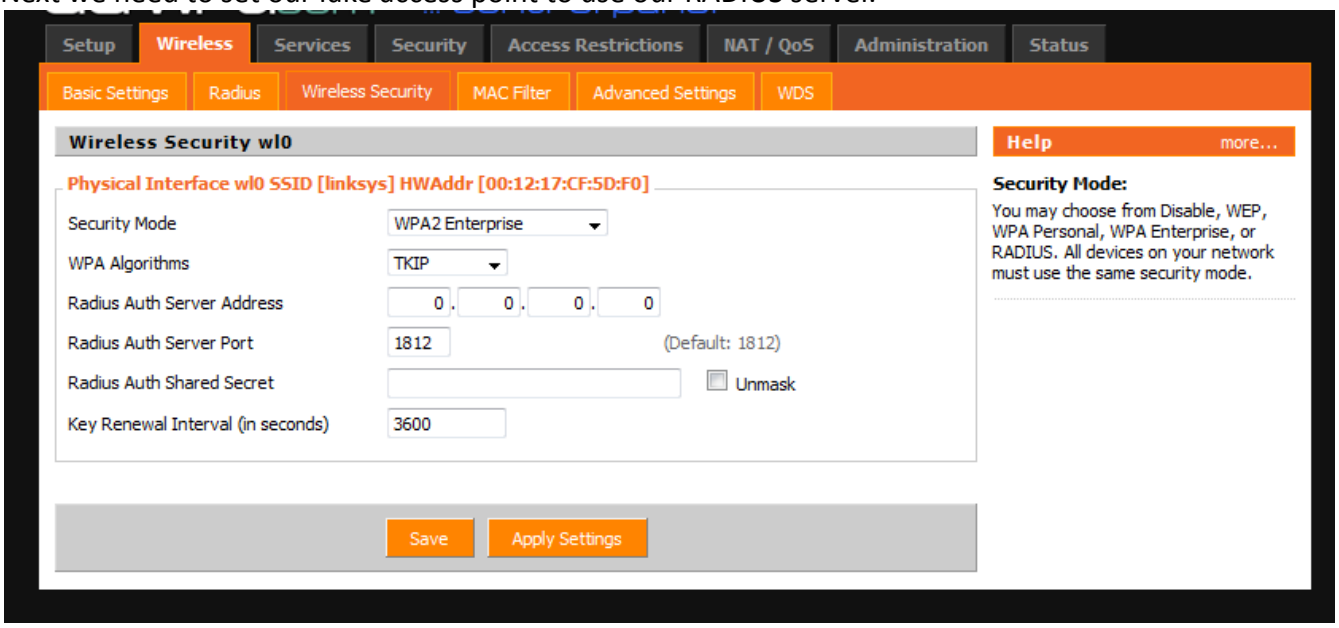
Start the server.

```
# radiusd
```

Monitor the Log File

```
# tail -f /usr/local/var/log/radius/freeradius-server-wpe.log
```

Next we need to set our fake access point to use our RADIUS server.



Fill in the required fields on the fake access point.

Now we need to get a client to connect to our AP. You can do this a few ways. You can simply wait until a client connects or if your impatient like me you can start deauthenticating people from legit access points. (we all know how to do that right :p) There's other ways as well, by having the strongest signal strength people will connect to your AP instead of others, you can do this by using antennas/amplifiers if necessary. Chances are you shouldn't have to go the amplifier route and you should have a victim connect to your AP and type in their credentials which the RADIUS server will capture. When viewing the log you should see something like this.

(**NOTE** VISIBLE ACCESS POINTS TAKE PRECEDENCE OVER HIDDEN ACCESS POINTS IN WINDOWS)

```
polonium radius # tail -f freeradius-server-wpe.log
mschap: Sat Feb  2 22:10:08 2008

        username: hrollins
        challenge: 08:92:54:d7:3c:33:c7:b7
        response: bb:6e:8f:4f:57:c8:da:71:3e:e4:91:a7:
dd:40:df:58:79:ac:5a:a9:53:36:05:ba
```

The challenge and response is their password. Now we have to crack it with a dictionary attack.

Fire up **Asleap**

This is what we will be using to crack the challenge and response. Type the following

```
./asleap -w "wordlistgoeshere" -C "Challenge" -R "Response"
```

Now you wait. Depending on how good your dictionary is you will have a password. GRATZ!

Scenario 2

(excuse my lack of detail, if anyone wants I will write up a more detailed version)

Now what if the certificate validation is used when configuring PEAP? This will cause the user to be prompted to accept the certificate when they join a new network. The dialog box that is presented gives VERY LITTLE DETAIL! Their certificate will verify that the network they are joining is correct and legitimate. We can apply the same attack as above and succeed as long as the user accepts the certificate and they did not specify which server the certificate is valid for which is not filled in by default. This is another very common negligence by people setting up PEAP. Now knowing end users, the chances are pretty good that they will click accept since the dialog provides minimal detail.

Now before we proceed we will need to sniff the certificate that the user is using. This can be done with almost any wireless capture tool. When a user connects to their network a TLS connection will be setup up and the certificate will be able to be captured as it is not encrypted during the first request. After some very basic wireless sniffing, determine the CA of the certificate. These are usually the major vendors such as Verisign. You will need to purchase a LEGITIMATE certificate from this vendor to perform the attack. After you have purchased the certificate set the fake RADIUS server up to use it. Now because the person who configured PEAP did not specify the server that the certificate was valid for the user will not see any difference in accepting ours since its from the same vendor.

Scenario 3
Iphone exploit

When you have a company that uses WPA/WPA2 enterprise chances are there's going to be some iphones around. This presents a great opportunity to infiltrate the network due to a fundamental flaw in the iphones wifi setup. The iphone does not have the options to specify what authentication type to use in regards to enterprise they simply just aren't there. The iphone also doesn't allow for a preconfigured certificates meaning they can't be tied to a legit RADIUS server. This flaw makes them susceptible even in the worst case scenario being certificate validation is enabled tied to a specific radius server. Please keep in mind that some phones do support these options, such as the Motorola droid but Iphones DO NOT.

Conclusion

When performing an audit on a WPA/WPA2 Enterprise network always check for common misconfiguration of their equipment as these may lead to insecurities. ALWAYS make sure your clients have certificate authentication enabled as well as a specific server tied to it.

Special Thanks to the guys over at SecureState

Well that's the end of this guide...I guess. Let me know what you think =)